CLAIMS

1. A method of communicating datagrams between terminals of a communication system, wherein each datagram comprises redundancy check data used to verify datagram integrity, the method comprising the steps of :

- generating (108) a first datagram comprising message data and first redundancy check data, which first redundancy check data is computed in dependence on the message data;
- sending (110) the first datagram from a first terminal to a second terminal;
- verifying the integrity of the first datagram;
- generating (126) a second datagram which comprises second redundancy check data, which second redundancy check data is computed in dependence on response data and first redundancy check data;
- sending (128) the second datagram from the second terminal to the first terminal;
- verifying the integrity of the second datagram;

and, in the case where the integrity of the second datagram is confirmed,

- identifying that the second datagram is the response to the first datagram.

2. A method according to Claim 1 wherein the step of verifying the integrity of the first datagram comprises the steps of :

- calculating third redundancy check data in dependence on the message data;
- comparing third redundancy check data with first redundancy check data; and
- determining the integrity of the first datagram in dependence on the comparison.

3. A method according to Claim 2 wherein the step of verifying the integrity of the second datagram comprises the steps of :

- calculating fourth redundancy check data in dependence on the response data and first redundancy check data;

- comparing fourth redundancy check data with second redundancy check data; and
- determining the integrity of the second datagram in dependence on the comparison.

4. A method according to Claim 1 wherein computing second redundancy check data comprises the steps of :

- initialising a first redundancy check data generator in dependence on the first redundancy check data;
- applying response data to the redundancy check data generator; and
- determining second redundancy check data in dependence on the value of the first redundancy check data generator.

5. A method according to Claim 1 or 4 wherein the step of verifying the integrity of the second datagram comprises the steps of :

- initialising a second redundancy check data generator in dependence on the first redundancy check data;
- applying response data of the second datagram and second redundancy check data to the generator, which response data was that used to compute the second redundancy check data; and
- determining the integrity of the second datagram in dependence on the value of the second redundancy check data generator.

6. A method according to any of Claims 1 to 5 wherein the second datagram further comprises the response data.

7. A communications system comprising a plurality of terminals, wherein each terminal employs the method of any of Claims 1 to 6.

8. A communications system as claimed in Claim 7, wherein the terminals are operable to communicate using datagrams defined in standard IEEE802.15.4.

9. A terminal for use in the communications system of any of Claims 7 to 8, and operable according to the method of any of Claims 1 to 6, the terminal comprising :

- a first port (202) operable to receive a datagram from another terminal;
- a processor (204) operable to:
  - decode a received datagram;
  - compute redundancy check data;
  - compare redundancy check data; and
  - generate a datagram;
- a first store (206) operable to store program code instructions;
- a second store (216) operable to store redundancy check data;
- a second port (212) operable to send datagrams to another terminal; and
- a third port (218) operable to exchange data with a host application.

10. A terminal according to Claim 9, in which the first store is non-volatile.

11. A terminal according to Claim 9, further comprising a redundancy check data generator.